AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE ACCOUNTS IDENTIFIED IN ATTACHMENT A, WHICH IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 3:19mj600

MICHAEL J. NEWMAN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(u)	Theft of firearms from a licensee
18 U.S.C. 922(j)	Possession of stolen firearms
18 U.S.C. 371	Conspiracy

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John D. Remick-Cook, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/8/19

Judge's signature

City and state: Dayton, Ohio

Hon. Michael J. Newman, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE ACCOUNTS IDENTIFIED IN ATTACHMENT A, WHICH IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	3:19mj600 [redacted] Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, John D. Remick-Cook, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google LLC accounts, identified as: **mike41sanford@gmail.com** ("SUBJECT ACCOUNT 1"), **trustnonmook@gmail.com** ("SUBJECT ACCOUNT 2"), **lamonthancock4@gmail.com** ("SUBJECT ACCOUNT 3"), and **dansbydion@gmail.com** ("SUBJECT ACCOUNT 4") (collectively the "SUBJECT ACCOUNTS"), as more fully described in Attachment A, which is stored at premises controlled by Google LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA, 94043. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the SUBJECT ACCOUNTS.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been so employed since March of 2015. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Glynco, Georgia. I also graduated from the ATF Special Agent

Basic Training Academy, located in Glynco, Georgia, in February of 2016. In my career with ATF, I have been assigned to and worked with the Cleveland Police Department's Gang Impact Unit and am currently assigned to an Organized Crime Task Force which investigates criminal organizations in the Southern Judicial District of Ohio. Prior to my employment with ATF, I was a member of the Metropolitan Police Department in Washington D.C. where I served as a member of the Third District Crime Suppression Team, Narcotics and Special Investigations Division's Gun Recovery Unit and as an Investigator with the Criminal Investigations Division. I was employed in that capacity from December of 2008 to March of 2015. I have received additional training in several areas of law enforcement, including but not limited to Gang investigations, Narcotics interdiction and investigation and firearms interdiction and investigation. I am also a graduate of the University of New Hampshire where I received two Bachelor degrees in Sociology and Justice Studies in 2008.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. § 922(u) (theft of firearms from a licensee); 18 U.S.C. § 922(j) (possession of stolen firearms); and 18 U.S.C. § 371 (conspiracy to commit the same), have been committed by Dion Dansby Jr., Lamont Hancock, Michael Sanford, and Miyauhn Vineyard. There is also probable cause to believe that evidence, fruits, and instrumentalities of these violations, as described more particularly in Attachment B, are present within the information associated with the SUBJECT ACCOUNTS.

PROBABLE CAUSE

5. On Sunday June 17, 2018, the ATF received a report that approximately 50 handguns were stolen during a break in at Target World, a Federal Firearms Licensee (FFL), located at 2300 Kemper Rd., Sharonville, Ohio.

6. At approximately 3:17 a.m., on June 17, 2018, five suspects were captured on surveillance video inside of Target World. Analysis of the crime scene showed that the suspects arrived in at least one vehicle which they parked on the east side of the McSwain Carpet & Floors (hereafter referred to as McSwain,) located at 2430 Kemper Rd., Sharonville, Ohio.

7. Surveillance footage recovered from Flavor Producers, located at 2429 Kemper Rd., Sharonville, Ohio 45241, showed two vehicles pulling into the parking area of McSwain shortly before the break in. The footage then showed two vehicles leave the parking lot shortly after the break in. The vehicles arrived together, but left at slightly different times. One of the vehicles can be seen turning off its headlights as it exited the McSwain parking lot.

8. Surveillance footage from McSwain showed a vehicle parked on the east side of the building, which then backed out of the camera's view shortly at around the time of the break in. The video then showed three suspects jumping a fence to gain access to the McSwain parking lot. Once the suspects gained access to the parking lot, they were able to travel across a set of train tracks, then an open field, bringing them to the east side of the Target World building.

9. Surveillance footage from Target World showed five suspects walking on the west side of the building lot and appears to show the group evaluating a door on the side of the building. The footage shows the suspects talking and, after a short time, the suspects travel northbound on the west side of the building toward the rear entrance to the range.

10. Surveillance footage from inside of the pistol range at Target World shows one of the suspects, who is wearing a bandana-type face covering, shorts, and a hooded sweatshirt with a design on both the front and rear, walk from the back of the range to the front. The suspect appears to scout the inside of the store by walking back and forth on the range. The suspect then appears to call for his co-conspirators to come to the front of the range, which they do. The footage shows that the remaining four suspects are wearing long pants and hooded sweatshirts with the hoods up and all are wearing facial coverings. Each individual is carrying a backpack or duffle-type bag.

11. Surveillance video shows that the suspects attempt to break a widow in the range using a hammer, but are unable to do so because the window is ballistic rated. The suspects then begin kicking the locked door, which leads from the range area to the retail portion of the store. After kicking the door several times, the suspects gain entry to the retail store and make entry. All five suspects then run over to the pistol case and break the glass on several cases. All five suspects can be seen reaching into the display cases and placing handguns into the bags that they brought along with them.

12. Within a matter of moments, the audible alarm sounded in the store and all five suspects fled the store the same way that they entered. Surveillance footage captured the suspects running along the west wall, then eastbound into the field toward McSwain's.

13. Officers from the Sharonville Police Department arrived on the scene within moments and discovered that a break in had occurred. The officers processed the crime scene and were able to determine the suspect's flight path prior to reviewing surveillance footage because the suspects dropped multiple firearms outside of the building as they fled. Specifically, firearms and sales tags were recovered in the Target World parking lot, the field between Target

World and McSwain's, the train tracks that run between Target World and McSwain's, and in McSwain's parking lot.

14. Responding officers also discovered a blood trail that traveled across McSwain's parking lot and blood smear on the side of McSwain's building and the chain link fence that the suspects jumped. The blood was collected from the scene and submitted to the Hamilton County Crime Lab (HCCL) for analysis.

15. On or about June 22, 2018, ATF Special Agent Timur Housum and ATF Task Force Officer (TFO) Joe Ruchti conducted an interview with ATF Source of Information (SOI) and were told the following:

a. SOI stated that on Monday, June 18, 2018, he/she had gone to 2926 Ralliston Ave. Dayton, Ohio 45417, which was a hangout area for him/her and associates. The SOI identified this location as "the clubhouse" and it will hereafter be referred to as such. While at the clubhouse, the SOI was told through conversation about a gun store being "hit." SOI identified five suspects as the subjects who had broken into the gun store by the following nicknames: "Lil D", "Lil Mike", Lamont, Joshua, and "Mook." SOI stated he/she was upset that they did not ask permission to do the burglary. SOI informed S/A Housum that he/she was the tactical advisor/enforcer for the group and that his/her associates would come for advice on how to "do stuff" to include burglaries/robberies. SOI stated that while at the clubhouse, he/she observed a red duffle bag with approximately 9-10 firearms in it. SOI stated he/she was told that each suspect that had a part in the burglary had grabbed two firearms each. SOI stated that the group gave him/her one of the firearms from the red duffle bag. The firearm received by the SOI is an uncommon firearm and is therefore somewhat recognizable.

b. SOI stated that he/she had sold the firearm for approximately $400.00, and had a photo of the firearm on his/her phone. S/A Housum reviewed the photo and recognized the firearm as being consistent with one of the more readily identifiable firearms taken during the burglary of Target World.

c. SOI went on to state that he/she assisted in a deal of approximately 8-9 firearms in the area of 2166 South Edwin C. Moses Boulevard, Dayton, Ohio, with two individuals. SOI stated that on June 19, 2018, he/she had received a phone call from an associate by the name of "TONE." In that phone call "TONE" stated that he needed SOI to pull into "ACES", later identified as Club Aces located near 2100 Nicholas Road, Dayton Ohio, because he (TONE), "had found some dudes to buy these guns." SOI and "TONE" met in the parking lot of Club Aces. "TONE" had parked his blue van and proceeded to hop into SOI's vehicle carrying what the SOI described as the same red duffle bag seen at the clubhouse the previous day with approximately 9-10 firearms in it. SOI stated "TONE" had wanted SOI there to watch "his back." "TONE" parked his blue van at the parking lot of Club Aces, and hopped in SOI's vehicle. SOI and "TONE" met up with an unknown black male in the parking lot of 2166 S. Edwin C. Moses Blvd. The unknown black male proceeded to grab the red duffle bag of firearms from SOI's vehicle and initiated the sale of firearms with two suspects. Once the deal was completed, SOI observed the unknown black male come back to his/her vehicle and hand "TONE" some cash. SOI stated "TONE" told him/her that he had sold the firearms for $1,200.00. After the deal was completed, SOI stated that he/she dropped "TONE" off at his vehicle at Club Aces. "TONE" stated he wanted SOI to follow him back to the clubhouse because "TONE" had money on him.

16. Later on June 22, 2018, S/A Housum and S/A Reed met with ATF SOI to identify associates. Upon review of pictures, SOI identified the following suspects: "Lil D" was identified by the SOI as Dion Dansby Jr., (black male, DOB: 04/XX/2000); "Lamont" was identified by the SOI as Lamont Hancock (black male, DOB: 04/XX/1999); Mook was identified by the SOI as Miyauhn Vineyard (black male, DOB: 11/XX/1999). Based on a physical description of "Mike" provided by the SOI, as well as open source database information and a photograph identified by the SOI as depicting "Mike," your Affiant believes based on this information that "Mike" is identified as Michael Sanford (black male, DOB: 11/XX/1994).

17. The SOI stated that Dansby Jr.'s cell phone number is 937-204-2251. The SOI stated that Hancock's cell phone number is 937-367-9473. The SOI stated that "Mike's" (Michael Sanford) cell phone number is 937-856-6960.

18. On October 19, 2018, and October 23, 2018, federal search warrants were issued authorizing the search of multiple Facebook accounts attributed to the suspected burglars. The returns of these warrants identified Google accounts belonging to the suspects. Specifically, a search of Michael Sanford's Facebook account revealed that he utilized the email address mike41sanford@gmail.com (SUBJECT ACCOUNT 1). Similarly, a search of Lamont Hancock's Facebook account revealed an associated email address of lamonthancock4@gmail.com (SUBJECT ACCOUNT 3). Finally, a return of Miyauhn Vineyard's Facebook account revealed an associated email address of trustnonmook@gmail.com (SUBJECT ACCOUNT 2).

19. A review of Lamont Hancock's Facebook account showed a conversation in June 2018 referencing hitting a "lick" at a gun store. I know based on my training and experience that

individuals involved in theft and burglary offenses use the term "lick" to describe the act of burglarizing or stealing.

20. On July 20, 2018, a federal search warrant was issued authorizing Agents to search the contents of cellular telephones belonging to Dion Dansby Jr., Michael Sanford, and Miyauhn Vineyard, which were in ATF custody. The search of Dion Dansby Jr.'s phone revealed that Dansby Jr. utilized the email account dansbydion@gmail.com (SUBJECT ACCOUNT 4) at the time of the burglary. The search of Miyauhn Vineyard's phone revealed photographs of three guns with serial numbers matching the serial number of guns stolen from Target World on June 17, 2018.

21. On or about June 26, 2018, Michael Sanford was involved in a traffic stop. Sanford was located in the passenger side of the vehicle. After the driver gave verbal consent to search the vehicle, a Glock firearm was found under the passenger seat of the vehicle. The Glock firearm was one of the firearms reported as stolen from Target World.

22. Based on the above, the theft from Target World referred to earlier in this affidavit involved multiple members and vehicles. Based on my training and experience as a law enforcement officer, I know that co-conspirators are frequently in phone contact with each other, passing information back and forth about timing and information about the particular locations involved in the offense, including ingress and egress routes and locations where getaway vehicles will be located.

23. I am also aware that such theft operations generally involve pre-operation surveillance. Specifically, the individuals planning the theft will typically visit the location at which they plan to conduct their theft prior to the theft's planned execution date/time in order to become familiar with the location's layout, entry and egress points, and the surrounding area (in

order to plan, e.g., primary and secondary routes out of the area). During such surveillance, which can take place several days in advance of the execution date, the individuals conducting surveillance are likely to utilize their cell phones to describe the scene to other conspirators or ask questions regarding the operation.

24. Based on my training and experience, I know that when people act in concert with one another to commit a crime, they frequently utilize cellular telephones to communicate with each other through voice calls, text messages, emails, and social media accounts. These cellular telephones allow them to plan, coordinate, execute, and flee the scene of crimes. Furthermore, I know people often take pictures utilizing their cellular telephones that may implicate them in a crime, i.e., possessing a firearm, posing with large quantities stolen items, or large amounts of cash.

25. Based on my training and experience, and the information provided herein, I know that individuals communicate about criminal conduct through social media accounts and access those social media accounts through cellular telephones. I also know that individuals engaged in illegal activity often maintain multiple email and social media accounts.

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

26. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about

what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

27. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet ("wi-fi") access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

28. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

29. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

30. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones,

known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

31. In addition, based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and Youtube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.

32. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

33. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist

for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

34. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device.

35. Based on my training and experience, I also known that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

36. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area

during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculpate or exculpate a Google account holder by showing that s/he was, or was not, near a given location at a time relevant to the criminal investigation.

37. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

38. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an

IP address, IP address information can help to identify which computers or other devices were used to access the account.

39. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Google user's IP log, stored electronic communications, and other data retained by Google, can indicate who has used or controlled the Google account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Google account at a relevant time. Further, Google account activity can show how and when the account was accessed or used. For example, as described herein, Google logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Google access, use, and events relating to the crime under investigation. Additionally, Google builds geo-location into some of its services. This geographic and timeline information may tend to either inculpate or exculpate the Google account owner. Last, Google account activity may provide relevant insight into the Google account owner's state of mind as it relates to the offenses under investigation. For example, information on the Google account may indicate the owner's motive and intent to

commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. Therefore, the computers of Google are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

42. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

John D. Remick-Cook
Special Agent
ATF

Subscribed and sworn to before me on this 8th day of October, 2019.

HON. MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Accounts identified as:

1. **mike41sanford@gmail.com**;

2. **trustnonmook@gmail.com**;

3. **lamonthancock4@gmail.com**; and

4. **dansbydion@gmail.com**

that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC ("Google"), regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period of **April 1, 2018 to present**:

a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

b. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above.

c. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the

subscribers, methods of payment, telephone numbers, addresses, change history, activity logs, device logs, and detailed billing and payment records.

e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

f. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

g. All existing printouts from original storage of all the electronic mail described above.

h. All account contents previously preserved by Google, in electronic or printed form, including all e-mail, including attachments thereto, and Google Drive stored electronic files for the account described above).

i. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above.

j. All associated YouTube viewing history, uploading history, and other content.

k. All location information stored in the Google account.

l. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

m. The types of service utilized;

n. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

o. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

Google is hereby ordered to disclose the above information to the government within fourteen days of service of this warrant.

II. Information to be Seized

All records of the Accounts described in Attachment A that relate to violations of:

- **18 U.S.C. § 922(u)**
- **18 U.S.C. § 922(j)**
- **18 U.S.C. § 371**

and involve **Dion Dansby Jr.**, **Lamont Hancock**, **Michael Sanford**, and **Miyauhn Vineyard** since **April 1, 2018**, including:

a. Any information related to the theft, purchase, use, or possession of firearms;

b. Any information related to the types, amounts, and prices of firearms stolen, purchased, used, or trafficked as well as dates, places, and amounts of specific transactions or theft;

c. Any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);

d. Any information regarding the location of Dansby, Hancock, Sanford, or Vineyard;

e. Any information regarding the location of the user of the Accounts;

f. All bank records, checks, credit card bills, account information, and other financial records;

g. Records of Internet Protocol addresses used;

h. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.